Remarks:

At the time of the outstanding Office Action, the pending claims in the application were claims 1-23. By this amendment, Applicant has (1) amended claims 1, 4-9, 11-15, 17, and 19-23, and (2) added new claims 45-64. No new matter is present. The pending claims are now claims 1-23 and 45-64. The independent ones of these claims are claims 1, 9, 20 and 53.

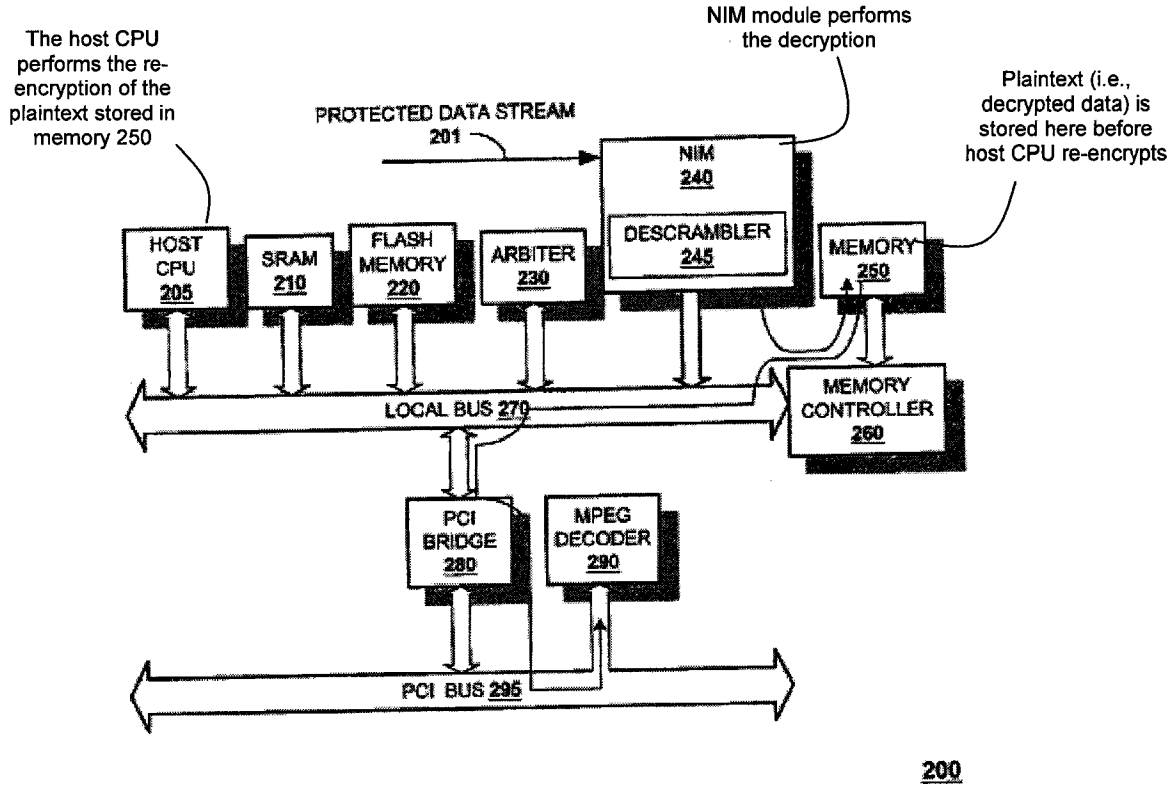
The Office Action rejected dependent claim 21 for allegedly reciting patent ineligible subject matter. While Applicant respectfully disagrees with this rejection, Applicant notes that the rejection has been rendered moot by virtue of the amendment to claim 21 which now recites a "key" rather than the "means for" language.

I. The independent claims are novel over Kovacevic.

The Office Action also rejected independent claims 1, 9 and 20 for alleged anticipation based on the Kovacevic reference (U.S. Pat. App. Pub. 2002/0150248). Applicant respectfully disagrees with this rejection.

Claim 1 recites a method where a reconfigurable logic device that bridges data transfers between a processor that requests the data transfers and a data store is used to provide secure trans-encryption such that decrypted data is not accessible to the processor. By virtue of the method of claim 1, the risk of a malware infection of the processor contributing to a data breach is minimized because the processor is not able to access the decrypted data, thereby enhancing data security. (See Patent Application at paragraphs 130-132 and 135 and Figures 37-39(b), with reference to this application's published version, U.S. Pat. App. Pub. 2007/0277036). Kovacevic fails to disclose the use of such a reconfigurable logic device.

Kovacevic describes as a primary embodiment a trans-encryption technique for encrypted video streams using a NIM module 240. Reproduced below is Figure 2 from Kovacevic that illustrates Kovacevic's primary embodiment. Kovacevic teaches that the NIM module be configured to decrypt a received "protected data stream" (e.g., a data stream that has been encrypted in some manner) and store the decrypted data (i.e., the plaintext) in memory 250. Thereafter, host CPU 205 re-encrypts the plaintext using a different encryption technique than was used to originally encrypt the data. (See Kovacevic; paragraphs 13-15; 23)



Therefore, in direct contradiction to claim 1, with this embodiment, Kovacevic does not prevent the processor from accessing the decrypted data. As such, this embodiment of Kovacevic fails to protect the decrypted data from malware that may infect the host CPU. Kovacevic merely teaches that by storing the plaintext in a memory 250 accessible only to a local internal bus 270 rather than the PCI bus 295 which can be accessed by external devices, the plaintext is safe from "external probing". By contrast, through the use of the reconfigurable logic device to perform the trans-encryption such that the decrypted data is not accessible to the processor, claim 1 is able to protect the decrypted data from internal malware that may be resident on the processor.

Furthermore, paragraph 19 of Kovacevic describes an alternate embodiment where the NIM module 240 can also be used to re-encrypt the decrypted data stream. However, Kovacevic is not clear as to where the decrypted data generated during the decryption operation would be stored. As such, Kovacevic fails to disclose that the decrypted data is not accessible to the host CPU (for example, Kovacevic could be interpreted as teaching that the NIM module should still store the decrypted data in memory 250 where it would be accessible to the host

CPU). Moreover, even if Kovacevic were interpreted as disclosing that the NIM module stores the decrypted data such that it is inaccessible to the host CPU, Applicant notes that Kovacevic fails to disclose that the NIM module can be deployed on a reconfigurable logic device, as required by claim 1. Kovacevic is simply silent regarding the use of a reconfigurable logic device, much less the use of a reconfigurable logic device to provide secure trans-encryption as recited in claim 1.

Therefore, Applicant respectfully submits that claim 1 is novel over Kovacevic. Furthermore, Applicant respectfully submits that independent claims 9, 20 and 53 are novel over Kovacevic for similar reasons.

Moreover, Applicant notes that the secondary reference, Ta (USPN 6,931,545), cited in the Office Action against various dependent claims of the patent application fails to bridge the gap between the independent claims and Kovacevic. Ta describes an Intellectual Property Rights Management (IPRM) system whereby an "integrity certification and verification device" is positioned between a content provider and a content consumer. Ta teaches that the role of the "integrity certification and verification device" is provide certification that applications and/or systems that are to receive the content from the content provider are acceptable to the content provider. While Ta states at col. 13, lines 45-59 that the "integrity certification and verification device" can be implemented on various types of reconfigurable logic devices (e.g., an FPGA), Ta does not use the "integrity certification and verification device" to provide trans-encryption of the subject content. Instead, Ta's "integrity certification and verification device" merely provides verification and authentication services with respect to consuming applications/systems so that the content provider can "trust" such consuming applications/systems. Therefore, Ta fails to bridge the gap between the independent claims and Kovacevic because Ta fails to contemplate the use of a reconfigurable logic device to provide secure trans-encryption.

Applicant further notes that other reasons exist for also finding the dependent claims patentable over the cited references, examples of which are elaborated upon below.

II. Dependent claims 46 and 58 are patentable over the cited references.

Dependent claim 46 recites that a "processing board in communication with the processor" comprises not only the "reconfigurable logic device" but also a "memory device that is not accessible to the processor", wherein the "reconfigurable logic device is further configured

to store the decrypted data only in the memory device." Claim 58 recites similar elements. Exemplary support for claims 46 and 58 can be found in the patent application at paragraphs 134-135 and Figure 39(a). Applicant notes that Kovacevic fails to disclose, teach or suggest this aspect of claims 46 and 58. Even assuming for the sake of argument that paragraph 19 of Kovacevic teaches that the NIM module 240 stores the decrypted data in memory 250, Applicant notes that this memory 250 is accessible to the host CPU 205, in direct contradiction to claims 46 and 58 and detracting from the data security of Kovacevic's system. Moreover, as stated above, Ta does not address trans-encryption issues and thus fails to even contemplate how decrypted data can be protected from malware that may be resident on a processor in a trans-encryption environment. For these reasons (as well as the reasons set forth above in connection with the independent claims), Applicant respectfully submits that dependent claims 46 and 58 are patentable over the cited references. Applicant further submits that dependent claims 4 and 11 are patentable over the cited references for similar reasons.

Further still, Applicant respectfully submits that dependent claims 47 and 59 are patentable over the cited references for reasons similar to those expressed above in connection with claims 46 and 58. Claim 47 recites that "the reconfigurable logic device includes internal memory that is not accessible to the processor" and further recites that the "reconfigurable logic device is further configured to store a portion of the decrypted data in its internal memory and store another portion of the decrypted data in the memory device [that is not accessible to the processor]". Claim 59 recites similar elements. Exemplary support for claims 47 and 59 can be found in the patent application at paragraph 134.

III. Dependent claims 49 and 61 are patentable over the cited references.

Dependent claim 49 further recites that the reconfigurable logic device employs a search engine to search "the decrypted data stream to find a targeted subset of the decrypted data in response to a data request", wherein the encryption operation is performed "by encrypting the targeted subset in the second encrypted format", and "wherein the data for sharing comprises the target data subset encrypted in the second encrypted format". Dependent claim 61 recites similar elements. Exemplary support for dependent claims 49 and 61 can be found in the application at paragraph 136. Thus, these claims define a reconfigurable logic device that serves as a secure search-enabled trans-encryption engine. Neither Kovacevic nor Ta contemplate such a capability. Therefore, for these reasons (as well as the reasons set forth

above in connection with the independent claims), Applicant respectfully submits that dependent claims 49 and 61 are patentable over the cited references.

Furthermore, Applicant respectfully submits that independent claim 53 is patentable over the cited references for similar reasons.

Conclusion

For the foregoing reasons, Applicant respectfully submits that all pending claims are in condition for allowance.

If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided below.

Furthermore, Applicant believes that this amendment and remarks are sufficient for overcoming the rejections raised by this Office Action. However, should Applicant later need to further respond to these or new claim rejections, Applicant reserves the right to fully respond to these and any other new rejections, including but not limited to further amending the claims and/or adding new claims, submitting evidence in favor of the patentability of the claims, disputing the alleged prior art status of the cited references if warranted, and raising new arguments in favor of patentability. Moreover, in submitting this response, Applicant does not acquiesce to any characterizations of the claims or art (including any characterizations about what is allegedly known in the art) made in the outstanding Office Action.

A speedy and favorable action is respectfully requested.

Respectfully submitted,

Benjamin L. Volk, Jr.
Reg. No. 48,017
Thompson Coburn LLP
One US Bank Plaza
St. Louis, Missouri 63101
(314) 552-6352
(314) 552-7352 (fax)

5231176